REMARKS

Claims 1-8 were pending in the application. The Examiner has rejected Claims 1-8 under 35 USC 101 as directed to non-statutory subject matter. Applicants respectfully disagree.

As is well understood by one having skill in the relevant art of encryption and communication of encrypted messages, parties each have a share of the "secret" which allows messages encrypted with a public key to only be decrypted by the owner of the corresponding private key. Accordingly a participating network device A can send and encrypted message, for example "encoded(m)" which has been encrypted using a public key of network device B. A message encrypted using the public key of network device B can be decrypted only by using B's private key, whereby (decoded(encoded(m))= m. Correspondingly, if B signs a message using B's private key, A will be able to decrypt the message using B's public key. When A and B are part of a synchronous network with all nodes connected along a proprietary broadcast channel, the sharing of keys is relatively safe and straightforward.

The present invention addresses the instance when nodes in an asynchronous network need to communicate along

non-trusted channels. Further, nodes in the asynchronous network may not be trusted (i.e., may be "faulty"), so that any receiving node must have a way to determine if the nodes are true or faulty based on the messages received from those nodes.

Calculating the RDA inverse function is required for authenticating messages/nodes. While encryption steps/calculations are included in the inventive method, the method is not simply generating numbers, but is exchanging secret information and performing node verification through the exchange of communications among the nodes. As such, the claimed steps are producing a "real world result" (MPEP, Chapter 2106, Section IV, part C).

Applicants respectfully submit that the present claims recite an inventive method which is statutory subject matter. Further, Applicants have amended the language of the independent claims to expressly recite that the exchanged information is used for authentication of messages among nodes in the asynchronous network.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendment, reconsideration of the rejections, and issuance of the claims.

Respectfully submitted,

Cachin

By: */Anne Vachon Dougherty/*
Anne Vachon Dougherty
Reg. No. 30,374
Tel. (914) 962-5910